

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 Claim 1 (Currently amended): Method for cryptographically  
2 processing data, comprising:  
3     a) feeding, to a cryptographic process (P), values,  
4         namely, the data (X) and a key (K), ~~and~~  
5     b) carrying out the process (P) in order to form  
6         cryptographically processed output data (Y),  
7         characterized by  
8     c) feeding, to the process (P), auxiliary values that  
9         mask the data (X) used in the process (P), ~~{K\*, A,~~  
10         ~~B)}~~ ~~and~~  
11     d) compensating, by an auxiliary process, the  
12         influence of the auxiliary values ~~to~~ on the output  
13         data (Y).  
14 ~~, in order to mask the values (K, D) used in the process~~  
15 ~~(P).~~

1 ~~Claim 2 (Currently amended): Method according to claim 1,~~  
2 ~~wherein an auxiliary value comprises a supplementary key~~  
3 ~~(K\*) which is fed to a supplementary process (P\*) in order~~  
4 ~~to form the key (K).~~ Method for cryptographically processing  
5 data, comprising;  
6     a) feeding, to a cryptographic process (P), values,  
7         namely data (X) and a key (K),

8        b) carrying out the process (P) in order to form  
9        cryptographically processed output data (Y),  
10       characterized by  
11       c) feeding, to a supplementary process (P\*), a  
12       supplementary key (K\*) in order to form the key (K),  
13       d) wherein the supplementary key (K\*) masks the key (K)  
14       used in the process (P), and  
15       e) wherein the supplementary process (P\*) comprises  
16       a cryptographic process to which an auxiliary  
17       key (K') is fed.

Claim 3 (Cancelled).

1       Claim 4 (Previously presented): Method according to  
2       claim 2, wherein the supplementary process (P\*) is an  
3       invertible process.

1       Claim 5 (Previously presented): Method according to  
2       claim 2, wherein the data (X) is also fed to the  
3       supplementary process (P\*).

1       Claim 6 (Original): Method according to claim 5, wherein  
2       carrying out the supplementary process (P\*) takes place  
3       exclusively if the data (X) has predetermined properties.

1       Claim 7 (Previously presented): Method according to  
2       claim 2, wherein the process (P) and the supplementary  
3       process (P\*) each are built up from a number of steps, and  
4       wherein steps of the process (P) and the supplementary  
5       process (P\*) are alternated.

1 Claim 8 (Currently amended): Method according to claim 1,  
2 wherein the process (P) comprises a number of steps ( $S_i$ ),  
3 each having a cryptographic operation ~~( $F_i$ ,  $F_i'$ ,  $F_i''$ )~~ for  
4 processing right-hand data ( $RD_i$ ) derived from the data (X)  
5 and a combinatory operation ( $C_i$ ) for combining with  
6 left-hand data ( $LD_i$ ) also derived from the data (X), the  
7 processed right-hand data ( $FD_i$ ) in order to form modified  
8 left data ( $SD_i$ ), and wherein the right-hand data ( $RD_i$ ) is  
9 combined with a primary auxiliary value ( $A_1$ ) prior to the  
10 first step( $S_1$ ) and the left-hand data( $LD_1$ ) is combined with  
11 an additional auxiliary value ( $A_0$ ).

1 Claim 9 (Original): Method according to claim 8 wherein,  
2 immediately after the last step ( $S_n$ ), the right-hand  
3 data ( $RD_n$ ) is combined with a further primary auxiliary  
4 value ( $A_n$ ) and the modified left-hand data ( $SD_n'$ ) is  
5 combined with a further additional auxiliary value ( $A_{n+1}$ ).

1 Claim 10 (Currently amended): Method according to claim 8,  
2 wherein the right-hand data ( $RD_i$ ) is combined, in each  
3 step ( $S_i$ ) and prior to ~~the~~ a cryptographic operation ( $F_i'$ ),  
4 with the primary auxiliary value ( $A_i$ ) of said step ( $S_i$ ).

1 Claim 11 (Currently amended): Method according to claim 10,  
2 wherein the processed right-hand data ( $FD_i$ ) is combined,  
3 following ~~the~~ a cryptographic operation ( $F_i$ ), with the  
4 secondary auxiliary value ( $B_i$ ) of said step ( $S_i$ ).

1 Claim 12 (Original): Method according to claim 11, wherein  
2 the secondary auxiliary value ( $B_i$ ) of a step ( $S_i$ ) is formed

from the combination of the primary auxiliary value ( $A_{i-1}$ ) of the preceding step and the primary auxiliary value ( $A_{i+1}$ ) of the next step.

Claim 13 (Previously presented): Method according to claim 8, wherein all primary auxiliary values ( $A_i$ ) are equal.

Claim 14 (Currently amended): Method according to claim 9, wherein the 25 primary auxiliary values ( $A_i$ ) and/or secondary auxiliary values ( $B_i$ ) have each time been combined with ~~the~~ a respective cryptographic operation ( $F_i$ ) in advance.

Claim 15 (Currently amended): Method according to claim 14, wherein a combined cryptographic operation ( $F_i'$ ) contains several tables, and wherein the tables are determined in a different order each time the process (P) is carried out.

Claim 16 (Currently amended): Method according to claim 14, wherein a combined cryptographic operation ( $F_i'$ ) contains several tables, and wherein the elements of the tables are determined and/or stored in a different order each time the process (P) is carried out.

Claim 17 (Original): Method according to claim 16, wherein the order is stored as a lookup table for the benefit of reading out the elements.

1 Claim 18 (Previously presented): Method according to  
2 claim 8, wherein the right-hand data ( $RD_i$ ) is combined with  
3 a tertiary auxiliary value ( $W_i$ ) after each step ( $S_i$ ).

1 Claim 19 (Original): Method according to claim 18, wherein  
2 the tertiary auxiliary value ( $W_i$ ) in all steps, except the  
3 last one ( $S_n$ ) is equal to the combination of the primary  
4 auxiliary value ( $A_1$ ) of the first step ( $S_1$ ) and the  
5 additional auxiliary value ( $A_0$ ), and in the last step ( $S_n$ )  
6 is equal to zero.

1 Claim 20 (Previously presented): Method according to  
2 claim 8, wherein combining is carried out using an XOR  
3 operation.

1 Claim 21 (Previously presented): Method according to  
2 claim 1, wherein the data (X) comprises identification data  
3 of a payment means (1) and the processed data (Y) forms a  
4 diversified key.

1 Claim 22 (Currently amended): Method according to claim 1,  
2 wherein the process (P) comprises DES, ~~preferably triple~~  
3 ~~DES.~~

1 Claim 23 (Previously presented): Circuit (10) for carrying  
2 out the method according to claim 1.

1 Claim 24 (Original): Payment card (1), provided with a  
2 circuit (10) according to claim 23.

1 Claim 25 (Original): Payment terminal (2) provided with a  
2 circuit (10) according to claim 23.

1 Claim 26 (New): Method according to claim 2, wherein the  
2 data (X) comprises identification data of a payment  
3 means (1) and the processed data (Y) forms a diversified  
4 key.

1 Claim 27 (New): Method according to claim 2, wherein the  
2 process (P) comprises DES.

1 Claim 28 (New): Circuit (10) for carrying out the method  
2 according to claim 2.

1 Claim 29 (New): Payment card (1), provided with a  
2 circuit (10) according to claim 28.

1 Claim 30 (New): Payment terminal (2) provided with a  
2 circuit (10) according to claim 28.

1 Claim 31 (New): Method according to claim 22, wherein the  
2 DES process is triple DES.

1 Claim 32 (New): Method according to claim 27,  
2 wherein the DES process is triple DES.